香港城市大學
City University of Hong Kong

電腦科學系
Department of
Computer Science

COMPUTER SCIENCE COLLOQUIUM

Authenticated and Private Data Feed to Smart Contract Using ZK-SNARK

SPEAKER **Prof Zhiguo WAN**

Associate Professor
School of Computer Science and Technology
Shandong University
China

DATE 29 November 2018(Thursday)
TIME 10:30 am - 11:30 am
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

The emerging blockchain technology, combined with the smart contract, is expected to revolutionize traditional systems by decentralization and autonomy. When the blockchain technology is applied in these systems, the blockchain may need to take in sensitive data to execute a smart contract. For example, a decentralized medical insurance smart contract needs access to personal health data. So it is crucial to guarantee privacy and authenticity of data sent to the blockchain, so that everyone can verify data without leaking sensitive information. Currently, only a few works have tried to achieve privacy and authenticity at the same time. In this work, we first propose zk-DASNARK, a zero-knowledge SNARK scheme for authenticated data. It is designed by combining the zk-SNARK technique with digital signature in an effective way. Based on zk-DASNARK, we design zk-AuthFeed, a zero-knowledge authenticated data feed scheme to achieve both data privacy and authenticity for blockchain based DApps (decentralized applications). We implement zk-AuthFeed and conduct comprehensive experiments on Ethereum. The experiments show that zk-AuthFeed is highly efficient: key generation takes about 7 seconds only, proof generation takes less than 2 seconds, and proof verification takes less than 40 ms.

BIOGRAPHY

Zhiguo Wan is the associate professor of the School of Computer Science and Technology, Shandong University since 2015. Before that, he was an assistant professor in School of Software Engineering, Tsinghua University. He has worked as a postdoc in K. U. Leuven, Belgium from 2006-2008. He obtained Ph.D. degree from National University of Singapore in 2007. He is a member of IEEE, ACM and China Computer Federation (CCF), and the founding member of the blockchain special committee of CCF. His research interests include security and privacy in blockchain, cloud computing, big data, IoT systems. He has published more than 40 research papers on academic conferences and journals including INFOCOM, IEEE TDSC, IEEE TIFS. He has been PC members for conferences including INFOCOM, GLOBECOM.

All are welcome!

In case of questions, please contact Dr Cong Wang at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/.